

Claims

What is claimed is:

1. A device, located at a remote site in communication with a network having at least one server, comprising:
 - a processor in communication with a memory, said processor operable to execute code for:
 - receiving a first information item comprising an access code and a content key scrambled using a key known by said remote site;
 - descrambling said first information item using a corresponding decrypting key; and
 - receiving a second information item scrambled using said content key after said server hosting the second information item verifies said access code.
2. The device as recited in claim 1, wherein said processor is further operable to execute code for:
 - descrambling said second information item using said content key.
3. The device as recited in claim 1, wherein said first information item includes a use-limit indication.
4. The device as recited in claim 1, wherein said processor is further operable to execute code for:
 - transmitting said unencrypted access code selected from the group consisting of: automatically, at a predetermined time, at a predetermined time offset, responsive to a manual input.
5. The device as recited in claim 1, wherein said known encryption key is selected from the group consisting of: a public key, a shared key.

6. The device as recited in claim 3, wherein said use-limit indication is selected from the group consisting of: number of uses, time-period.
7. The device as recited in claim 1, wherein said first information item further includes a content location.
8. The device as recited in claim 7, wherein said processor is further operable to execute code for transmitting said content location.
9. The device as recited in claim 1, wherein said content location is known.
10. A method, operable at a receiving device located at a remote site in communication with a network having at least one server, for descrambling secure content received over said network, said method comprising the steps of:
 - receiving a first information item comprising an access code and a content key scrambled using a key known by said remote site;
 - descrambling said first information item using a corresponding decrypting key; and
 - receiving a second information item, scrambled using said content key after the server hosting the second information verifies said access code; and
 - descrambling said second information item using said content key.
11. The method as recited in claim 10, wherein said first information item includes a use-limit indication.
12. The method as recited in claim 10, wherein said known encryption key is selected from the group consisting of: a public key, a shared key.
13. The method as recited in claim 11, wherein said use-limit indication is selected from the group consisting of: number of uses, time-period.
14. The method as recited in claim 10, wherein said first information item further includes a content location.

15. The method as recited in claim 14, wherein said content location is known.
16. A method for transferring secure content over a network comprising the steps of:

receiving a request for content at a first server over a first network from a file requesting device, said request including an encryption key known to a designated remote site;

generating a first information containing a content access credential and a content key at said server; and

transferring said first information item to said designated remote site having a file receiving device, wherein said content access credential and said content key are scrambled using said encryption key.

17. The method as recited in claim 16, further comprising the steps of:

transferring over a second network said secure content after verification of said content access credential, wherein said secure content is encrypted using said content key.

18. The method as recited in claim 16, wherein said first network and said second network are the same network.
19. The method as recited in claim 16, wherein said file requesting device is selected from the group consisting of: personal digital assistant, cellular telephone, notebook computer and personal computer.
20. The method as recited in claim 16, wherein said file receiving device is selected from the group consisting of: personal digital assistant, cellular telephone, notebook computer and personal computer.
21. The method as recited in claim 16, wherein said first network is a wireless network.

22. The method as recited in claim 16, wherein said first information item includes a location of said content.
23. The method as recited in claim 16, further comprising the step of:
 - transmitting said content to at least one other server in communication with said first server, wherein said content is scrambled using said content key.
24. The method as recited in claim 23, further comprising the steps of:
 - transferring over a second network said secure content after verification of said content access credential, wherein said secure content is scrambled using said content key.
25. The method as recited in claim 16, wherein the step of transferring said content access credential and said content key is over said first network.
26. The method as recited in claim 16, wherein the step of transferring said content access credential and said content key is over said second network.
27. The method as recited in claim 16, wherein said second network is a high-speed network.
28. The method as recited in claim 27, wherein said second network is a content delivery network.
29. The method as recited in claim 16, further comprising the step of:
 - transferring a location of said content to said designated remote site.